AF/2132/#

Practitioner's Docket No. NAI1P094/02.013.01 *PATENT*

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Joseph J. Pantuso et al.

Application No.: 10/071,549 Group No.: 2132
Filed: 02/08/2002 Examiner: Zand, Kambiz
For: FIREWALL SYSTEM AND METHOD WITH NETWORK MAPPING CAPABILITIES

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 1.192)

1. Transmitted herewith, in triplicate, is the APPEAL BRIEF in this application, with respect to the Notice of Appeal filed on May 27, 2004.

2. STATUS OF APPLICANT

This application is on behalf of other than a small entity.

CERTIFICATION UNDER 37 C.F.R. §§ 1.8(a) and 1.10*
*(When using Express Mail, the Express Mail label number is **mandatory**;*
Express Mail certification is optional.)

I hereby certify that, on the date shown below, this correspondence is being:

MAILING

✓ deposited with the United States Postal Service in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

37 C.F.R. § 1.8(a)
✓ with sufficient postage as first class mail.

37 C.F.R. § 1.10*
_ as "Express Mail Post Office to Addressee"
Mailing Label No. _____ **(mandatory)**

TRANSMISSION

_ facsimile transmitted to the Patent and Trademark Office, (703) _____ - _____.

Erica L. Farlow
Signature

Date: 5/28/04

Erica L. Farlow
(type or print name of person certifying)

** Only the date of filing (' 1.6) will be the date used in a patent term adjustment calculation, although the date on any certificate of mailing or transmission under ' 1.8 continues to be taken into account in determining timeliness. See ' 1.703(f). Consider "Express Mail Post Office to Addressee" (' 1.10) or facsimile transmission (' 1.6(d)) for the reply to be accorded the earliest possible filing date for patent term adjustment calculations.*

3. FEE FOR FILING APPEAL BRIEF

Pursuant to 37 C.F.R. § 1.17(c), the fee for filing the Appeal Brief is:

other than a small entity $330.00

Appeal Brief fee due $330.00

4. EXTENSION OF TERM

The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5. TOTAL FEE DUE

The total fee due is:

Appeal brief fee	$330.00
Extension fee (if any)	$0.00

TOTAL FEE DUE $330.00

6. FEE PAYMENT

Attached is a check in the amount of $330.00.

A duplicate of this transmittal is attached.

7. FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAI1P094).

Signature of Practitioner

Reg. No.: 41,429
Tel. No.: 408-971-2573
Customer No.: 28875

Kevin J. Zilka
Silicon Valley IP Group, PC
P.O. Box 721120
San Jose, CA 95172-1120
USA

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the application of	)
	)
Pantuso et al.	) Group Art Unit: 2132
	)
Application No. 10/071,549	) Examiner: Zand, Kambiz
	)
Filed: February 08, 2002	) Dct. No. NAI1P094/02.013.01
	)
For: FIREWALL SYSTEM AND METHOD WITH NETWORK MAPPING CAPABILITIES	) Date: May 28, 2004)

Commissioner for Patents
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPELLANT'S BRIEF (37 C.F.R. § 1.192)

This brief is in furtherance of the Notice of Appeal, filed in this case on May x, 2004.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief is transmitted in triplicate. (37 C.F.R. § 1.192(a))

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 1.192(c)):

I REAL PARTY IN INTEREST

II RELATED APPEALS AND INTERFERENCES

III STATUS OF CLAIMS

IV STATUS OF AMENDMENTS

V SUMMARY OF INVENTION

VI ISSUES

VII GROUPING OF CLAIMS

VIII ARGUMENTS

APPENDIX OF CLAIMS INVOLVED IN THE APPEAL

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 1.192(c)(1))

The real party in interest in this appeal is Networks Associates Technology, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 1.192(c)(2))

With respect to other appeals or interferences that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals or interferences.

III STATUS OF CLAIMS (37 C.F.R. § 1.192(c)(3))

A. TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1-29.

B. STATUS OF ALL THE CLAIMS IN APPLICATION

1. Claims withdrawn from consideration but not canceled: None
2. Claims pending: 1-29
3. Claims allowed: None
4. Claims rejected: 1-29

C. CLAIMS ON APPEAL

The claims on appeal are: 1-29

IV STATUS OF AMENDMENTS (37 C.F.R. § 1.192(c)(4))

As to the status of any amendment filed subsequent to final rejection, there are no such amendments after final.

V SUMMARY OF INVENTION (37 C.F.R. § 1.192(c)(5))

A method and computer program product are provided for tracing a traffic event utilizing a firewall. As set forth in Figure 3 and the accompany description, a firewall is executed on a local computer. See operation 301 of Figure 3. Moreover, traffic events between the local computer and a remote computer over a network are monitored utilizing the firewall. See operation 302 of Figure 3. As set forth in Figure 6 and the accompanying description, the traffic events are displayed utilizing the firewall. Moreover, at least one of the traffic events is traced utilizing the firewall. Further, a world map is displayed with an illustration of the trace thereon utilizing the firewall.

VI ISSUES (37 C.F.R. § 1.192(c)(6))

Issue # 1: The Examiner has rejected Claims 1-29 under 35 U.S.C. 103(a) as being unpatentable over Maloney et al. (U.S. Patent No. 6,269,447) in view of Dev et al. (5,261,044).

VII GROUPING OF CLAIMS (37 C.F.R. § 1.192(c)(7))

The claims of the following groups do not stand or fall together. Following is the grouping of claims. In the following section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1: Grouping of Claims –

Group #1: Claims 1-25, and 28.

Group #2: Claim 26.

Group #3: Claim 27.

Group #4: Claim 29.

VIII ARGUMENTS (37 C.F.R. § 1.192(c)(8))

Issue #1:

The Examiner has rejected Claims 1-29 under 35 U.S.C. 103(a) as being unpatentable over Maloney et al. (U.S. Patent No. 6,269,447) in view of Dev et al. (5,261,044).

Group #1: Claims 1-25, and 28

With respect to the Group #1, appellant respectfully disagrees with this rejection, since the Examiner's proposed combination is deficient in many respects.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck,*947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991). Appellant respectfully asserts that at least the first and third elements of the *prima facie* case of obviousness have not been met.

With respect to the first element of the *prima facie* case of obviousness, the Examiner states that it would have been obvious to one of ordinary skill in the art at the time of the invention was made to utilize Dev et al.'s multiple views such as a world map view in Maloney's information security analysis and monitoring network system. Appellant respectfully disagrees with this assertion, especially in view of the vast evidence to the contrary.

For example, Maloney relates to an information security analysis system, while Dev relates to a computer network management system. To simply glean features from a computer network management system, such as that of Dev, and combine the same with the *non-analogous art* of information security analysis systems, such as that of Maloney, would simply be improper. Computer network management systems manage parameters such as performance and a status of network components, while an information security analysis system mitigates Internet security issues.

"In order to rely on a reference as a basis for rejection of an appellant's invention, the reference must either be in the field of appellant's endeavor or, if not, then be reasonably pertinent to the particular problem with which the inventor was concerned." In re Oetiker, 977 F.2d 1443, 1446, 24 USPQ2d 1443, 1445 (Fed. Cir. 1992). See also In re Deminski, 796 F.2d 436, 230 USPQ 313 (Fed. Cir. 1986); In re Clay, 966 F.2d 656, 659, 23 USPQ2d 1058, 1060-61 (Fed. Cir. 1992) In view of the vastly different types of problems a computer network management system addresses as opposed to an information security analysis system, the Examiner's proposed combination is inappropriate.

Moreover, it is noted that Maloney discloses a "tree-based" node representation, such that a count of nodes is an aggregate of all nodes below the reference node. Moreover, the tree-based approach provides for browsing objects in classes within the knowledgebase. If one were to attempt to utilize the geographical map of Dev in the context of Maloney's "tree-based" node representation, Maloney would no

longer be able to provide "a count of nodes [that] is an aggregate of all nodes below the reference node," as well as provide tree-based object browsing.

Thus, any attempt to combine the geographical map of Dev in the context of Maloney's "tree-based" node representation would *modify/frustrate the intended function/purpose* of Maloney, and is thus improper. See *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

Thus, Dev clearly *teaches away* from the teachings of Maloney. *In re Hedges*, 783 F.2d 1038, 228 USPQ 685 (Fed. Cir. 1986).

In response to these arguments, in the Examiner's latest action, the Examiner argues that both Dev and Maloney deal with a network environment that consists of nodes or devices that can be connected as a WAN; and management of a network involves security such as a firewall, encryption, passwords, access and security analysis to ensure the integrity of the network.

In response, it appears that the Examiner has generalized and broadened the description of the Dev and Maloney inventions to avoid their paramount differences, and to lump the two very different inventions together in the art of "network environments." Appellant asserts that this is improper, especially since appellant has pointed out the very different problems which both inventions address. See supra.

Further, it appears that the Examiner has only addressed appellant's *non-analogous art* arguments, but has failed to address the foregoing *modify/frustrate the intended function/purpose* and *teaching away* arguments.

More importantly, with respect to the third element of the *prima facie* case of obviousness, the Examiner's proposed combination fails to disclose, teach or suggest all of appellant's claim limitations.

For example, with respect to appellant's claimed "displaying a world map with an illustration of the trace thereon utilizing the firewall," the Examiner states the following: Maloney teaches "where after the analysis of an event[, a] map of the trace is displayed," and "Dev ... display[s] a network world map of network events..."

Maloney, however, merely suggests "a visual interface for the knowledge base 16 and provides a tree-based approach to browsing objects in classes within the knowledge base, and in addition provides linkage information for tracing items and information passively discovered on the network by the discovery tool" (see col. 8, lines 42-46).

Thus, contrary to the Examiner's assertion, this disclosure does not even suggest that a map of the trace is displayed. Instead, there is merely a suggestion that "linkage information" is provided utilizing "a visual interface." There is simply no display of a map of a trace, as purported by the Examiner.

Moreover, further contrary to the Examiner's assertion, Dev displays a network world map of network entities (i.e. devices), not events, as claimed by appellant.

Thus, the third element of the *prima facie* case of obviousness has not been met, since the proposed combination fails to meet appellant's claimed "displaying a world map with an illustration of the trace thereon utilizing the firewall" (emphasis added).

In response to these arguments, in the Examiner's latest action, the Examiner points to the same excerpts from Maloney and Dev to make a prior art showing of appellant's claimed "displaying a world map with an illustration of the trace thereon utilizing the firewall." For the reasons set forth hereinabove, appellant asserts that

the Examiner's rejection is deficient, and the third element of the *prima facie* case of obviousness has not been met.

Group #2: Claim 26

With respect to the Group #2, appellant respectfully disagrees with the foregoing rejection, since the Examiner's proposed combination is deficient in many respects.

With respect to the first element of the *prima facie* case of obviousness set forth above, appellant asserts that such element has not been met for the reasons set forth hereinabove.

Further, with respect to the third element of the *prima facie* case of obviousness, the Examiner's proposed combination fails to disclose, teach or suggest all of appellant's claim limitations.

Specifically, with respect to appellant's claimed "displaying a plurality of nodes of the network segments upon the selection of a second one of the views utilizing the firewall" and "displaying a list of the network segments upon the selection of a third one of the views utilizing the firewall," the Examiner relies on cols. 4-11 and col. 12, lines 1-34 of Maloney to make a prior art showing of such limitations.

However, Maloney fails to disclose, teach or even suggest a combination of second and third views selectable to show a plurality of nodes of the network segments and a list of the network segments, upon the selection thereof. As a collateral matter, it appears that the Examiner mis-cited appellant's claim limitations on page 8 of the final office action mailed 04/22/04 by not acknowledging that appellant teaches and claims a view including a list of the network segments, in combination with the remaining claim elements.

For the reasons set forth hereinabove, appellant asserts that the Examiner's rejection is deficient, and the third element of the *prima facie* case of obviousness has not been met.

Group #3: Claim 27

With respect to the Group #3, appellant respectfully disagrees with the foregoing rejection, since the Examiner's proposed combination is deficient in many respects.

With respect to the first element of the *prima facie* case of obviousness set forth above, appellant asserts that such element has not been met for the reasons set forth hereinabove.

More importantly, with respect to the third element of the *prima facie* case of obviousness, the Examiner's proposed combination fails to disclose, teach or suggest all of appellant's claim limitations.

Specifically, with respect to appellant's claimed "wherein the event log identifies a time...associated with the traffic events" and "organizing the traffic events in the event log based on times the traffic events are logged utilizing the firewall," the Examiner relies on the following excerpts from Maloney to make a prior art showing of such limitations.

> "For example, router and firewall software can be monitored in near real time to determine if the code has been functionally changed regardless of security precautions. LAN/WAN data contained in the protocols from the Data Link to Presentation layers in the OSI model are available for analysis with associated displays in two and three-dimensional space." (col. 2, lines 27-29)

Such excerpt, however, fails to disclose, teach or even suggest "wherein the event log identifies a time ... associated with the traffic events" and "organizing the traffic

events in the event log based on times the traffic events are logged utilizing the firewall." Appellant contends that the mere mention of a time period or "real-time" does not rise to the level of specificity required by the foregoing claim limitations.

For the reasons set forth hereinabove, appellant asserts that the Examiner's rejection is deficient, and the third element of the *prima facie* case of obviousness has not been met.

Group #4 – Claim 29

With respect to the Group #4, appellant respectfully disagrees with the foregoing rejection, since the Examiner's proposed combination is deficient in many respects.

With respect to the first element of the *prima facie* case of obviousness set forth above, appellant asserts that such element has not been met for the reasons set forth hereinabove.

More importantly, with respect to the third element of the *prima facie* case of obviousness, the Examiner's proposed combination fails to disclose, teach or suggest all of appellant's claim limitations.

Specifically, the Examiner has not even made an attempt to make a prior art showing of appellant's claimed "wherein the trace is shown to involve a plurality of displayed network segments shown to be spanning different cities of different countries displayed on the world map." The Maloney-Dev proposed combination fails to disclose, teach or even suggest any sort of trace that is shown to involve a plurality of displayed network segments shown to be spanning different cities of different countries displayed on the world map.

For the reasons set forth hereinabove, appellant asserts that the Examiner's rejection is deficient, and the third element of the *prima facie* case of obviousness has not been met.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

IX APPENDIX OF CLAIMS (37 C.F.R. § 1.192(c)(9))

The text of the claims involved in the appeal is:

1. (Previously Amended) A method for tracing a traffic event utilizing a firewall, comprising:

(a) executing a firewall on a local computer;

(b) monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;

(c) displaying the traffic events utilizing the firewall;

(d) tracing at least one of the traffic events utilizing the firewall; and

(e) displaying a world map with an illustration of the trace thereon utilizing the firewall.

2. (Original) The method as recited in claim 1, wherein the traffic events are displayed in an event log.

3. (Original) The method as recited in claim 2, wherein the event log identifies a time and an Internet Protocol (IP) address associated with the traffic events.

4. (Original) The method as recited in claim 2, wherein the traffic events are organized based on times the traffic events are logged.

5. (Original) The method as recited in claim 2, wherein the traffic events include attempts to access the local computer.

6. (Original) The method as recited in claim 1, wherein the at least one traffic event is traced in response to a user request.

7. (Original) The method as recited in claim 1, wherein the tracing includes identifying a plurality of network segments traversed by the traffic event.

8. (Original) The method as recited in claim 7, wherein the map includes the network segments.

9. (Previously Amended) The method as recited in claim 8, and further comprising displaying a plurality of views.

10. (Original) The method as recited in claim 9, wherein a geographical location of the network segments is displayed upon the selection of a first one of the views.

11. (Original) The method as recited in claim 10, wherein nodes of the network segments are displayed upon the selection of a second one of the views.

12. (Original) The method as recited in claim 11, wherein a list of the network segments are displayed upon the selection of a third one of the views.

13. (Previously Amended) A computer program product for tracing a traffic event utilizing a firewall, comprising:

(a) computer code for executing a firewall on a local computer;

(b) computer code for monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;

(c) computer code for displaying the traffic events utilizing the firewall;

(d) computer code for tracing at least one of the traffic events utilizing the firewall; and

(e) computer code for displaying a world map with an illustration of the trace thereon utilizing the firewall.

14. (Original) The computer program product as recited in claim 13, wherein the traffic events are displayed in an event log.

15. (Original) The computer program product as recited in claim 14, wherein the event log identifies a time and an Internet Protocol (IP) address associated with the traffic events.

16. (Original) The computer program product as recited in claim 14, wherein the traffic events are organized based on times the traffic events are logged.

17. (Original) The computer program product as recited in claim 14, wherein the traffic events include attempts to access the local computer.

18. (Original) The computer program product as recited in claim 13, wherein the at least one traffic event is traced in response to a user request.

19. (Original) The computer program product as recited in claim 13, wherein the tracing includes identifying a plurality of network segments traversed by the traffic event.

20. (Original) The computer program product as recited in claim 19, wherein the map includes the network segments.

21. (Previously Amended) The computer program product as recited in claim 20, and further comprising computer code for displaying a plurality of views.

22. (Original) The computer program product as recited in claim 21, wherein a geographical location of the network segments is displayed upon the selection of a first one of the views.

23. (Original) The computer program product as recited in claim 22, wherein nodes of the network segments are displayed upon the selection of a second one of the views.

24. (Original) The computer program product as recited in claim 23, wherein a list of the network segments are displayed upon the selection of a third one of the views.

25. (Previously Amended) A system for tracing a traffic event utilizing a firewall, comprising:

(a) logic for executing a firewall on a local computer;

(b) logic for monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;

(c) logic for displaying the traffic events utilizing the firewall;

(d) logic for tracing at least one of the traffic events utilizing the firewall; and

(e) logic for displaying a world map with an illustration of the trace thereon utilizing the firewall.

26. (Previously Amended) A method for tracing a traffic event utilizing a firewall, comprising:

(a) executing a firewall on a local computer;

(b) monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;

(c) displaying the traffic events utilizing the firewall;

(d) tracing at least one of the traffic events utilizing the firewall;

(e) displaying a geographical location of a plurality of network segments associated with the traffic event on a world map upon the selection of a first one of a plurality of views utilizing the firewall;

(f) displaying a plurality of nodes of the network segments upon the selection of a second one of the views utilizing the firewall; and

(g) displaying a list of the network segments upon the selection of a third one of the views utilizing the firewall.

27. (Previously Amended) A method for tracing a traffic event utilizing a firewall, comprising:

(a) executing a firewall on a local computer;

(b) monitoring traffic events between the local computer and a remote computer over a network utilizing the firewall;

(c) logging the traffic events in an event log utilizing the firewall, wherein the event log identifies a time and an Internet Protocol (IP) address associated with the traffic events;

(d) organizing the traffic events in the event log based on times the traffic events are logged utilizing the firewall;

(e) displaying the traffic events in the event log utilizing the firewall;

(f) detecting the selection of one of the traffic event by a user;

(g) tracing at least one of the traffic events utilizing the firewall upon the selection thereof, wherein the tracing identifies a plurality of network segments traversed by the traffic event;

(h) detecting the selection of one of a plurality of views by the user; and

(i) displaying the network segments in the selected view upon the selection of one of the views, wherein one of the views includes a world map with an illustration of a trace thereon.

28. (Previously Amended) A method for geographically tracing a traffic event utilizing a personal firewall, comprising:

monitoring traffic events between a local computer and a remote computer over a network utilizing a personal firewall;

displaying the traffic events in an event log utilizing the personal firewall, wherein the traffic events are organized based on a time associated therewith;

tracing at least one of the traffic events utilizing the personal firewall; and

displaying the trace on a world map utilizing the personal firewall,

wherein the at least one traffic event is traced in response to a user request.

29. (Previously Amended) A computer program product for geographically tracing a traffic event utilizing a personal firewall, comprising:

computer code for monitoring traffic events between a local computer and a remote computer over a network utilizing a personal firewall;

computer code for displaying the traffic events in an event log utilizing the personal firewall, wherein the traffic events are organized based on a time associated therewith;

computer code for tracing at least one of the traffic events utilizing the personal firewall; and

computer code for displaying the trace on a world map utilizing the personal firewall,

wherein the at least one traffic event is traced in response to a user request;

wherein the trace is shown to involve a plurality of displayed network segments shown to be spanning different cities of different countries displayed on the world map.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P094/02.013.01).

Respectfully submitted,

By: _____ Date: 5/25/04

Kevin J. Zilka

Reg. No. 41,429

Silicon Valley IP Group, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660